



# התכנלה ללימודי מקצועות הסייבר

## התכנית ללימודי מקצוע מנהל טכנולוגיות הגנת סייבר



# CYBER MAN

# CYBER WOMAN

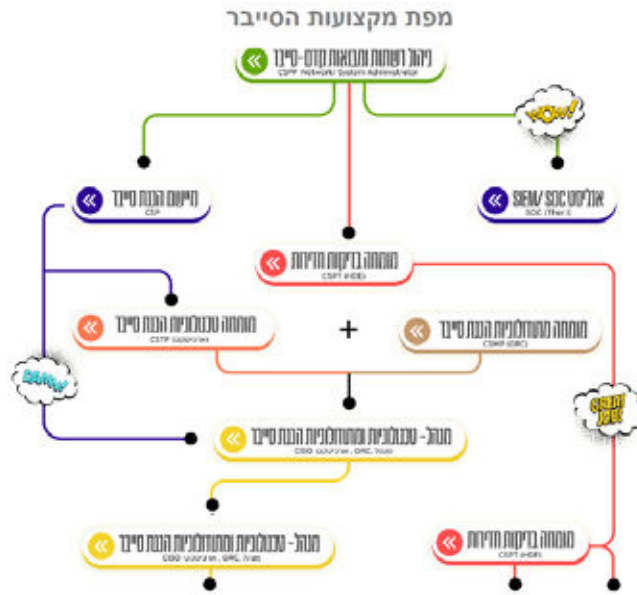


## מנהל טכנולוגיות הגנת סייבר (CSP)

תכנית זו מיועדת  
לבעלי רקע נרחב  
בתשתיות

התוכנית נועדה להכשיר אנשי hands-on בעלי רקע טכנולוגי יישומי עשיר  
לניהול משימות הגנת סייבר בארגונים. התוכנית מאופיינת במעבדות  
מתקדמות, אשר מלוות את הנושאים התיאורטיים. הנושאים זוקקו והתואמו  
לדרישות מעסיקים בישראל.

מאושר על ידי משרד הכלכלה  
לפיקודן חיילים משוחררים  
ולתוכנית השוברים



## להיות מנהל טכנולוגיות הגנת סייבר.

מנהל טכנולוגיות הגנת סייבר אחראי על תכנון מענה טכנולוגי, תוך שילוב טכנולוגיות ושיטות אבטחה,  
התאמת מוצרי הגנה ושילובם וליווי אירועי אבטחה מתוך הבנת הפעילות, הצרכים והמטרות הארגונית,  
הכל- לצורך הגנת הסייבר בארגון.

ולא פחות חשוב: נלמד בפּי שָׂרָק שִׂיא סְקוּיִרִיטִי יוֹדַעַת לְלַמֵּד: נכּוֹן, וְעַם הַלֵּב.



# התכנית ללימודי מקצוע מנהל טכנולוגיות הגנת סייבר (CSP)

התוכנית נבנתה בהתאם לאסדרת מקצועות הסייבר בישראל ועבור הסמכה הבינלאומית Security+

מאפייני תוכנית הלימודים	
עלות:	15,500 שח + 400 שח דמי הרשמה
קהל:	מנהלים / סביבתיים / מקצוענים
אוריינטציה:	מנהלית/ טכנית / יישום
מטרה:	הכשרת אנשי Hands-on של טכנולוגיות אבטחת מידע איכותיים, עתירי ידע.
שלב:	בעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת).
רוחב:	ממוקד / רחב
עומק:	סוקר / עמוק
הסמכות:	CompTIA Security+ or: (ISC) <sup>2</sup> SSCP
שעות:	155 שעות
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	הלימודים בקמפוס המכללה ברמת גן, מתקיימים פעמיים בשבוע בימי בערב: 17:30 עד 21:30 (5 שעות אקדמיות למפגש), במשך כ-5 חודשים
תרגול בית:	בהיקף כ-200 שעות

הגנת סייבר (CSMP: Cyber Security Methodology Professional), מומחה בדיקות חדירות (Hacker/Penetration Tester), ומומחה חקירות (Forensics). תכנית זו הינה שילוב CSTP ו- CSMP – כמפורט ונכלל בתכנית זו.

### סגנון לימוד

טכני, Hands-on, ותיאורטי.

### מעבדות תרגול בינלאומיות

תכנית זו הינה עתירת תרגול מעשי במעבדות בינלאומיות מתקדמות המיועדות גם לתרגול מבית התלמיד.

### עלות

סך 15,500 שח + 400 שח דמי רישום (כולל מע"מ).

### אודות המכללה

מכללת See Security הנה מכללה בינלאומית התמחותית למקצועות ניהול רשתות וסייבר, אחת מ-7 מכללות מסוגה בעולם ומהמוערכות שבהן, ועוסקת בלעדית בתחום זה בכל זמנה, במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים.

המכללה מייצאת את תכניות הלימודים לכל רחבי העולם, באמצעות המותג See Security International, ובאמצעות גופי סייבר ישראלים ידועי-שם העוסקים ביצוא בטחוני.

מנהל הקבוצה שבה משולבת המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר, יועץ לממשלת ישראל בנושא "אסדרת מקצועות הגנת הסייבר" בישראל, פרשן בערוצי השידור בארץ ובחו"ל, מקימו של הפורום הלאומי לאבטחת מידע IFIS יחד עם האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרו, מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר - SeeHR, בחברה ליעוץ See Consulting – Cyber, בחברה לפתרונות See Secure – Managed SEIM/SOC, ובמכללה הבינלאומית לסייבר See Security College International.

### אודות תוכנית הלימודים

התוכנית נועדה להכשיר אנשי hands-on בעלי רקע טכנולוגי יישומי עשיר לניהול משימות הגנת סייבר בארגונים. התוכנית מאופיינת במעבדות מתקדמות, אשר מלוות את הנושאים התיאורטיים. הנושאים זוקקו והתואמו לדרישות מעסיקים בישראל.

הדרישה ההולכת וגוברת למומחי הגנת סייבר משכילים ובעלי ידע, מחייבת רקע רחב ועמוק במיוחד, במסגרת מתודולוגית סדורה אשר תאפשר השתלטות על המידע הרב, וזו מהות המסלול.

מערך הסייבר פרסם בינואר 2015 רשימה רשמית למקצועות ליבה, ובהם: מיישם הגנת סייבר (CSP: Cyber Security Practitioner), מומחה טכנולוגיות הגנת סייבר (CSTP: Cyber Security Technology Professional), מומחה מתודולוגיות



### קהל יעד

למעוניינים להתמחות כמיישמי הגנת סייבר, או להמשיך למקצועות מוסמך טכנולוגיות הגנת סייבר, ונדרשים להכשרת מיישמי הגנת סייבר כדרישת סף לקראת ההכשרה במקצועות אלו בהמשך לימודיהם. [ראה בסוף המסמך: מפת התפתחות מקצועית בענף הסייבר].

### דרישות סף

- ידע וניסיון בתחום התשתיות (סיסטם ותקשורת).
- אנגלית ברמה טובה.
- ראיון אישי לבחינת ההתאמה לתכנית.

### מתכונת הלימודים

משך התכנית 155 שעות כיתה, ו-200 שעות משימות (סך הכל 355 שעות), פעמיים בשבוע בערב בשעות 17:30 עד 21:30 במשך כ-5 חודשים, 5 שעות אקדמיות למפגש. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז).

### חובות אקדמיות

קיימת חובת נוכחות ב-80% מהמפגשים. קבלת תעודת המכללה מותנית בעמידה במבחני מעבר, בציון 70 לפחות (מבחן חוזר ללא תשלום). בנושאים הטכניים - תרגול (Hands-on) בכיתה ובבית.

### זכאות לתעודה והסמכות בינלאומיות

לעומדים בדרישות התכנית תוענק תעודת הסמכה יוקרתית מטעם המכללה:

### "CSP: Cyber Security Practitioner"

בנוסף להסמכות הבינלאומיות כמפורט (+Security או SSCP) לתלמידים אשר ניגשים עצמאית לאחר השלמת חוק לימודיהם במכללה.

מי שאינם עומדים בדרישות יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום.

### כיצד נבנה המוניטין של המכללה?

מנקודת המבט של הנהלת המכללה, תלמיד מצליח אך ורק אם הצליח להשתלב אצל מעסיק בתפקיד רלוונטי. לכן הגדרת תכני הקורס נבנתה בהתאם לדרישת המעסיקים.

המעסיק דורש ומצפה כי בוגר של מכללה ייעודית לסייבר כמו See Security יגיע בוגר יותר, עשיר יותר ובעל ידע רב תחומי, ויחזיק ברשותו גם הסמכה בינלאומית מוכרת באופן רשמי.

"המתחרה" של המועמד איננו המעסיק. להיפך: הוא מבקש את הטוב ביותר לעצמו. כאשר הוא מבקש לקלוט מועמד של



## מה אני עושה לאחר סיום הלימודים? הצעד הבא

בסיום הקורס תוכל לבחור מהו הצעד הבא שלך:

1. להתחיל לעבוד כמיישם סייבר.

2. להמשיך בצעד הבא - תכנית הלימודים CSTP - ארכיטקט הגנת סייבר.



3. להמשיך בצעד הבא - תכנית הלימודים CSPT - מומחה בדיקות חדירות (האקר, מבוסס על תכנית הלימודים הבינלאומית Hacking Defined Experts).



אנו ממליצים כי תבקש פגישת יעוץ עם אבי ויסמן, בין אם הנך משדרג מעמך מעולם ה-IT, ובין אם הנך מבקש ליזום הסבה מקצועית.

### בוגרי ובוגרות מכללת שיא סקורירטי?

קבלו מיועצי הלימודים הצעה מיוחדת.

### לתשומת ליבך!

תהליך הייעוץ והסינון של היועץ האקדמי משמעותי לבחינת סיכויך להצליח במסלול זה ו/או במסלולים אחרים, ובעתידך התעסוקתי בכלל.

### הערות

- ההרשמה לכל מבחן חיצוני, הנה בתשלום ותבוצע באחריות הסטודנט בלבד.
- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.

מכללה מקצועית-ייעודית, הוא מצפה לפחות שיהיה בעל ידע רב יותר ממועמד המגיע מחברות אחרות המשוקקות קורסים.

### סגל המרצים

תכנית לימודים כל-כך מולטי-דיסציפלינארית ובכירה, מחייבת שימוש נרחב ובלתי מתפשר במומחים יעודיים, איש לתחומו. על המרצים נמנים מובילי הענף, בהם: מנהלי סייבר ידועי שם, ומומחים מקצועיים המובילים בתחומם. כמדינה הנוטלת על עצמה להוביל את הגנת הסייבר בעולם, רואה עצמה המכללה מחויבת לדרישות גבוהות ולסטנדרט גבוה מאוד של מרצים.

### מה אנחנו מצפים מבוגר התכנית?

1. בתקופת הלימודים תשקיע את כל הזמן כדי לקיים את הנחיות המרצה, אינך הראשון ולא תהיה האחרון שימצא עצמו מיישם הגנת סייבר בלב התעשייה.
2. בסיום לימודיך היעזר בהנהלת המוסד לבניית טופס קורות חיים ההולם את מאמציך.
3. הסתפק בתחילת דרכך במשרה רלבנטית מכל סוג שהוא כדי לצבור ניסיון (נסה לעשות זאת כבר בתקופת הלימודים).
4. בדוק עם היועץ האקדמי את איכות עמידתך בריאיון אישי לקראת ראיונות העבודה האמיתיים, במקרים מסויימים אפילו תלמיד מצטיין זקוק לתיקונים (פשוטים יחסית) שמשביחים מאוד את יכולתו למצוא משרה איכותית.
5. צא לדרכך, אל תשכח להמשיך ללמוד, דאג תמיד להיות מבחינת ידע רמה אחת יותר מהאחרים, כי ככל שתגביה כך יהיו לך פחות מתחרים, שכר גבוה יותר, וסיפוק רב יותר.

### תוכנית לימודים לדוגמה בעמודים הבאים:

- המכללה מביאה לידיעת הנרשמים והסטודנטים, כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.



## תוכנית קורס אינטגרטור - מנהל טכנולוגיות הגנת סייבר (CSP)



מס'	נושא ראשי	שם השיעור	נושאי השיעור
1	Introduction to Cybersecurity	פתיחת הקורס והיכרות, סקירת הנושאים הנלמדים בקורס, הצגת עולם ב-Cyber Security ו-CASE STUDIES	השיעור הראשון בקורס, נועד לייצר אוריינטציה והכוונה לתלמידים לקראת המשך הקורס: * היכרות עם מנהל הקורס * היכרות עם אדמיניסטרציית הקורס (מערכת LMS, ערוצי קשר עם המכללה, עדכניות לוו"ז) * הצגת הדרישות/חובות במהלך הקורס.
2		יסודות בעולם הסייבר ואבטחת המידע [שיעור כפול]	* מונחים ומושגי יסוד * בקרת גישה (Access Control) לרבות בעולם הפיזי, ברשתות, במערכות הפעלה. עיקר המיקוד יעשה סביב שני צירים משיקים - (1) הזדהות, אימות והרשאות (כהקדמה לעולם ה-2); (IAM) הגבלת גישה בתקשורת. * עקרונות אבטחת מידע (הצורך בידיעה, עקרון ההרשאה המינימלית, זיכוי משאבים משותפים)
3		יסודות בעולם הסייבר ואבטחת המידע [שיעור כפול]	* נושאים בקריפטוגרפיה - בדגש תעודות דיגיטליות ומערכי PKI
4		מבוא להתמודדות עם איומי סייבר [שיעור כפול]	היכרות עם השיטות והכלים הקיימים להתמודדות קטגוריות עם איומי סייבר. * מתודולוגיית MITRE ATT@CK MATRIX (כולל Workshop) * עולם ה-Anti-Malware - מושגים (סוגי Malware), שיטות להתמודדות (Signature, Heuristics, Protocol Deviations, Behavioral / Contextual)
5		מבוא להתמודדות עם איומי סייבר [שיעור כפול]	* עולם ה-Firewall - סקירה מהירה של האבולוציה מ-Packet Filter ל-Stateful Inspection והדגשת הפערים בין הגנה (או פעילות) בשכבות OSI השונות (הצגת עולם ה-Network Firewall vs. Application Firewall) * עולם ה-IDPS - התייחסות גם ל-Intrusion Detection וגם ל-Intrusion Prevention. * ההבדל בין Host-IDPS (ו Host-FW) לבין Network-IDPS (ו Network-FW).
6		Cybersecurity and the Business	היכרות עם עולם הכספים.

### לא לומד? אל תתפלא.



## תוכנית קורס אינטגרטור - מנהל טכנולוגיות הגנת סייבר (CSP)

7	אבטחת רשתות תקשוב (והגנה על מערכות תקשורת) - Network Security. מיקוד במצופה ממישם הגנת סייבר ככל שמדובר במערכות להגנת הרשת (והגנת רכיבי הרשת). * כניסה לעולם ההקשחות.	אבטחת רשתות תקשוב (אבטחת הרשת ואבטחת הרכיבים)
8	הקשחת מערכות הגנה רשתיות (הגנה על המערכות עצמן). תרגול מעשי של הגדרות הקשחה ברכיבים מכוננים (למשל Firewall, מתג או נתב) והצגת המשמעות של הקשחה לא מתאימה או לקויה. בין היתר, תרגול נושאים כגון: * ניהול מבוסס Out of Band - מתן גישה ניהול למקורות מסוימים (Access Control List) * ניהול משתמשים (מקומי / מרכזי) - והמשמעויות של שימוש במשתמש קבוצתי ידוע לכולם * כיבוי שירותים שאינם נדרשים - והמשמעויות של השארת שירותים נגישים (למשל SNMP)	הקשחת מערכות הגנה רשתיות (הגנה על המערכות עצמן)
9	תרגול בכיתה (ובמקביל גם לפחות פי 2 שעות לתרגול בית) של הגדרת תצורה עבור Checkpoint Firewall (בהתאם לגרסאות. כרגע R81). הכרת המוצר וכיולו לתצורה הבסיסית ביותר המאפשרת עבודה ברשת ומכאן להתחיל ולתרגל שינויים ב-Policy תוך שינוי Wireshark ובאמצעות ניסוי וטעייה.	Checkpoint Firewall - תרגול הגדרות תצורה לרכיבי רשת תוך ניסוי וטעייה בתרחישים
10	הגדרות תצורה לרכיבי רשת תוך ניסוי וטעייה בתרחישים	תרגול
11	תרגול בכיתה (ובמקביל גם לפחות פי 2 שעות לתרגול בית) של הגדרת תצורה עבור Fortigate Firewall (בהתאם לגרסאות. כרגע 7.0.1). הכרת המוצר וכיולו לתצורה הבסיסית ביותר המאפשרת עבודה ברשת ומכאן להתחיל ולתרגל שינויים ב-Policy תוך שינוי Wireshark ובאמצעות ניסוי וטעייה.	Fortigate Firewall - תרגול הגדרות תצורה לרכיבי רשת תוך ניסוי וטעייה בתרחישים
12	אבטחת עמדות ומערכות הפעלה System Security בסביבות Microsoft. מותאם לידע הנדרש בהסמכת +Security.	אבטחת עמדות ומערכות הפעלה
13	התמודדות עם הגדרות הקשחה שונות ברמת Active Directory ו-GPO.	תרגול הקשחות מערכות הפעלה ושרתים (בדגש ACTIVE DIRECTORY ו-GPO) - חלק 1
14	התמודדות עם הגדרות הקשחה שונות ברמת Active Directory ו-GPO.	תרגול הקשחות מערכות הפעלה ושרתים (בדגש ACTIVE DIRECTORY ו-GPO) - חלק 2
15	התמודדות עם פריסה, התקנה והגדרה של רכיבי Endpoint Security.	תרגול כלים טכנולוגיים (EDR/ANTI-VIRUS) התקנות ותפעול
16	תרגול הרחבה	SYSTEM SECURITY
17	תרגול מעשי	עולם ה- Regular Expression
18	הכרות עם עולם ה-Scripting	Powershell
19	תרגול פרקטי בעולמות Windows (ניהול / בקרה)	Powershell

### לא לומד? אל תתפלא.



## תוכנית קורס אינטגרטור - מנהל טכנולוגיות הגנת סייבר (CSP)

עולם אירועי הסייבר ואבטחת המידע (מושגים והגדרות, כלים וטכנולוגיות), הצגת עולם ה-SOC	20	Cybersecurity Incident Management Infrastructure - On Premise
עולם ה-Syslog, עיבוד נתוני יומן (Parsing)	21	
הכרות עם מערכות SIEM	22	
הבנת עולם ההתרעות, חוקי יסוד, חוקי קורלציה, חיפוש מידע	23	
מערכות SIEM SPLUNK - חלק 1	24	
מערכות SIEM SPLUNK - חלק 2	24	Cybersecurity Incident Management Infrastructure - On Cloud
תרגול	25	
הכרה של סביבות ענן וסביבות היברידיות	26	
מערכת SIEM, יומני מערכות ושילובן בענן - 1	27	
מערכת SIEM, יומני מערכות ושילובן בענן - 2	27	Cybersecurity Incident Handling and Response
מערכת SIEM, יומני מערכות ושילובן בענן - 3	28	
חיפוש ממוקד במערכות SIEM ובניית מודעות מצבית	29	
Cyber security and the Business	עיוני	30
מרתון הכנה למבחן ההסמכה Security+	Security +	31-38

סה"כ: 190 שעות אקדמיות\*

\* ייתכנו שינויים בתוכנית השיעורים ובנושאי הלימוד



לא לומד? אל תתפלא.